European Cyber Security Challenge

Simulation des Ernstfalls

Daniel Marth

- Student Technische Universität Wien
- Catalysts
  - security@catalysts.cc
  - Software Entwickler: https://www.catalysts.cc/
  - Penetration Tester: https://www.catalysts.cc/pentest/
- Cyber Security Challenge Austria
- European Cyber Security Challenge

Cyber Security Challenge Austria

- Nationaler IT-Security Wettbewerb
- Cyber Security Austria
- Ziel: Finden und fördern von Talenten
- Ablauf
  - Einzelqualifikation
  - Vorbereitung im Team
  - Finale

Einzelqualifikation

- Online
  - Hacking-Lab
- ~4 Monate
- Monatlich neue Aufgaben
- “Jeopardy Style”

Vorbereitung im Team

- 2 Kategorien
  - 14-20 Jahre
  - 21-30 Jahre
- Top 10 je Kategorie im Finale
- 2 Teams je Kategorie (Auslosung)
- Teamtrainer des Bundesheeres
  - Teambuilding
  - Präsentationstechnik
  - Strategie

Finale

- Team gegen Team je Kategorie
- Lösen der Aufgaben im Team
- Präsentation einer Aufgabe vor Jury
- Ab 2013: Siegerteams beider Kategorien => **Team Austria**

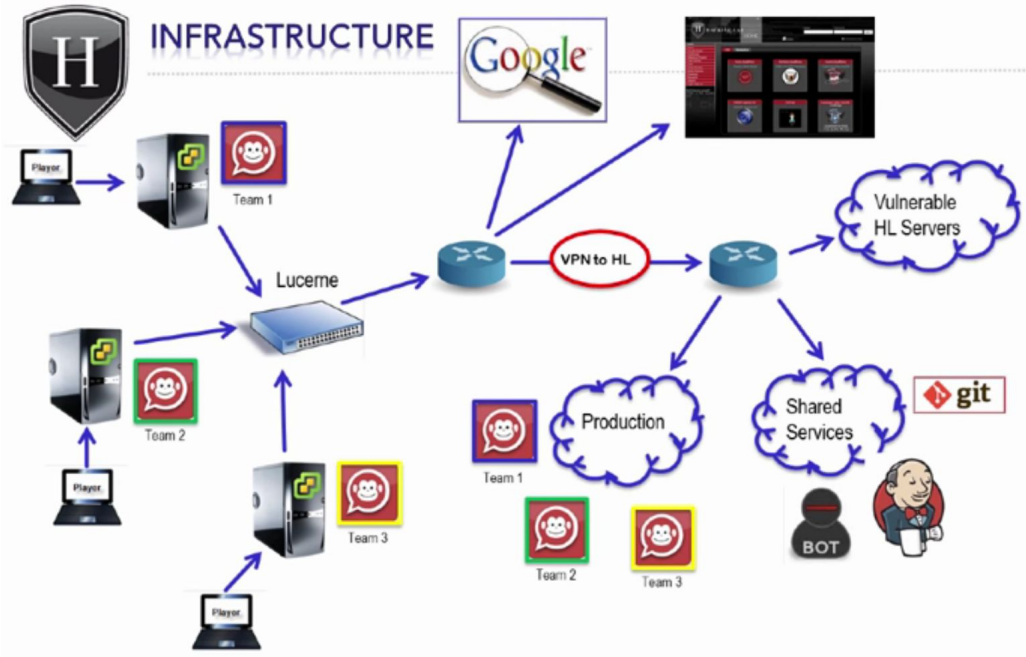

AUSTRIA
CYBER SECURITY
CHALLENGE
Du bist verboten gut?
CYBER SECURITY
AUSTRIA
Five Years Out
IKARUS
security software
NTT Communications
A1
BRZ
Systems
SPARKASSE
BM.I
ÖSTERREICH
StaDt Wien
www.verbotengut.

European Cyber Security Challenge

- Wettbewerb zwischen mehreren europäischen Nationen
- Ziel: Internationale Vernetzung
- 2013: Österreich, **Schweiz** (“Alpen Cup”)
- 2014: **Österreich**, Schweiz, Deutschland
- 2015: **Österreich**, Schweiz, Deutschland, Großbritannien, Rumänien, Spanien

Ausgangslage

- Wesentlich komplexere Infrastruktur
- Attack-Defense
- Alle Teams in 1 Raum
- Signalton




EUROPEAN
CYBER SECURITY
CHALLENGE
Evil prevails when good humans do nothing!

Szenario 2015

- Jede Nation repräsentiert Firma
- Rollen
  - CEO
  - CTO
  - Press Officer
  - Engineers
- Firma wird angegriffen

Aufgaben

- Fehler in eigener Infrastruktur beheben
- Fehler in fremder Infrastruktur ausnutzen
- Presseberichte
- Klassische (“Jeopardy Style”) Aufgaben
- Fehlertoleranz bei Totalausfall der Infrastruktur

Strategie

- Eigene Hardware
- Verantwortliche für virtuelle Infrastruktur
- Backup der kompletten virtuellen Infrastruktur
- Administrator Zugriff
- Angriff > Verteidigung > Jeopardy
- Kleinteams (2-3 Personen) bilden

Probleme

- Fehlerhafte Bewertung der Angriffspunkte
- Teilweise zentralisiertes Wissen über Infrastruktur

EUROPEAN CYBER SECURITY CHALLENGE

Evil prevails when good humans do nothing!

Strategien für den Tag danach

- Vorbereitung
  - Verantwortliche für System
  - Interne Vernetzung
- Analyse der Situation
- Fehler beheben
- Maßnahmen treffen
- Offenheit gegenüber Kunden / Partnern

Kontakt / Links

- security@catalysts.cc

- http://www.cybersecuritychallenge.at/
- http://www.europeancybersecuritychallenge.eu/
- https://www.hacking-lab.com/